ครรชิต มาลัยวงศ์

ไวรัสคอมพิวเตอร์

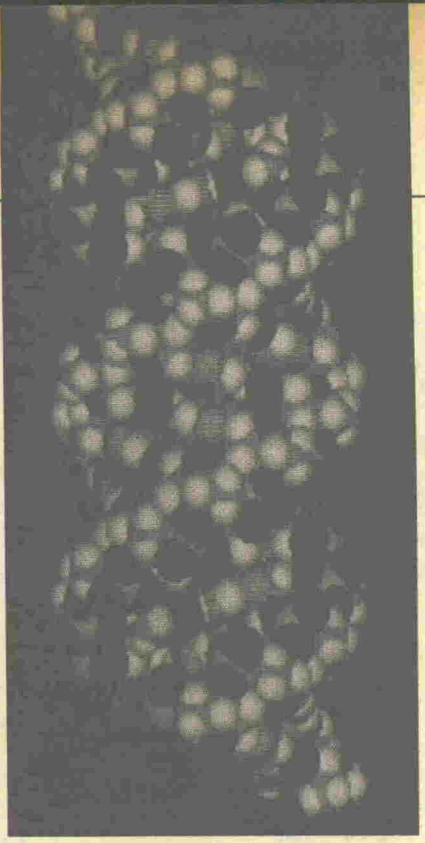
"ลักษณะของไวรัสคอมพิวเตอร์ก็คือ
ชุดคำสั่งที่สามารถก๊อบปี้ตัวเองเข้าไปในโปรแกรมอื่นๆ ได้
เมื่อบรรจุลงในคอมพิวเตอร์ หรือข่ายงานคอมพิวเตอร์
มันจะสามารถหาตำแหน่งที่อยู่ใหม่ได้เอง"

เมื่อกลางเดือนกุมภาพันธ์ที่ผ่านมานี้ ผมได้มีโอกาสไปร่วมประชุมวิชาการเรื่องการประยุกต์ใช้คอมพิวเตอร์ในงานวิศวกรรมที่มหาวิทยาลัยสงขลานครินทร์ ระหว่างมีการประชุมนั้นนอกจากผมจะได้พบเพื่อนเก่ามากมายหลายคนแล้ว ผมยังได้มีโอกาสปล่อยไก่ตัวโตด้วย แต่บังเอิญมีคนเห็นไม่กี่คนเท่านั้น

เรื่องของเรื่องมีอยู่ว่าอาจารย์ท่านหนึ่งถามผมว่า "ได้ข่าวว่าที่เอไอทีมีปัญหาเรื่องไวรัสคอมพิวเตอร์หรือครับ"

ผมสะดุ้งเล็กน้อยและพยายามไม่ให้อาจารย์ท่านนั้นสังเกตได้ ไม่ใช่เพราะเอไอทีมีไวรัสคอมพิวเตอร์ระบาดดอกครับ แต่เป็นเพราะผมไม่ทราบจริงๆ ว่า อะไรคือไวรัสคอมพิวเตอร์ ก่อนลงไปใต้ผมเคยเห็นพาดหัวข่าวบางกอกโพสต์เรื่องนี้เป็น ซ้ำเคยมีอาจารย์คนหนึ่งเปรยขึ้นในที่ประชุมด้วยว่าไวรัสคอมพิวเตอร์ทำลายแผ่นดิสเกตต์ของเราไปหลายแผ่นแล้ว แต่ผมก็ไม่สนใจซ้ำยังเห็นว่าเป็นไปไม่ได้ด้วยที่จะมีการทำลายดิสเกตต์แบบนั้น สงสัยจะเป็นเพราะซื้อแผ่นดิสเกตต์ที่ไม่ได้มาตรฐานมากกว่า

เมื่อเกิดอคติขึ้นมาอย่างนั้นผมก็อธิบายว่าผมไม่ค่อยเชื่อเรื่องไวรัสคอมพิวเตอร์เท่าใดนัก แต่ครั้นเมื่อผมกลับมาถึงกรุงเทพฯแล้ว ผมก็พบสำเนาสารบัญวารสารคอมพิวเตอร์ต่างๆ ที่ทางห้องสมุดเพิ่งได้รับวางอยู่บนโต๊ะของผม และเมื่อผมลองพลิกดูก็พบ



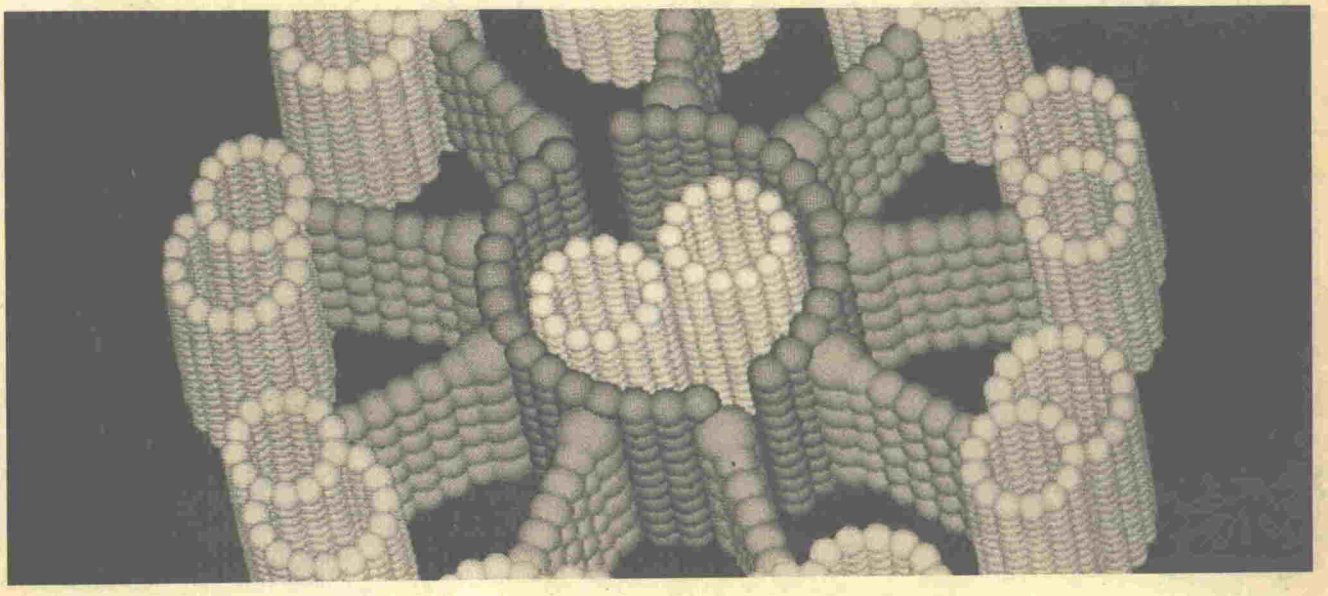
เห็นชื่อบทความเรื่องเกี่ยวกับไวรัสคอมพิวเตอร์ตีพิมพ์ในวารสาร Systems and Software ฉบับเดือนธันวาคมปีที่แล้วนี้เอง

ผมรีบตามหาบทความเรื่องนี้มาอ่านด้วยความสนใจ เมื่ออ่านเสร็จก็ต้องรีบเปลี่ยนทัศนคติเกี่ยวกับเรื่องไวรัสคอมพิวเตอร์ในทันที โดยเฉพาะที่คิดว่าเรื่องนี้เป็นเรื่องเหลวไหลนั้น ถ้าจะไม่จริงเสียแล้ว และคงจะต้องหาทางป้องกันตนเองเอาไว้ด้วย ซึ่งจะทำอย่างไรนั้นก็ขอให้ลองพิจารณาเนื้อหาของบทความซึ่งผมขอนำมาถ่ายทอดให้ท่านผู้อ่านได้รับทราบบ้าง บทความนี้ชื่อ Recovering from a Computer Virus Attack ของ F.G.F. Davis และ R.E. Gantenbein แห่งมหาวิทยาลัยไวโอมิงในสหรัฐอเมริกา

ผู้เขียนทั้งสองกล่าวว่าการแทรกซึมโจมตีระบบคอมพิวเตอร์นั้นอาจทำได้หลายวิธี วิธีที่ใช้กันมาเก่าแก่ก่อนใครเพื่อนก็คือโปรแกรมม้าโทรจัน ซึ่งได้ชื่อมาจากม้าไม้ขนาดใหญ่ที่ใช้ในการตีกรุงทรอย โปรแกรมนี้เขียนโดยผู้ใช้ธรรมดาๆ ที่ได้รับอนุญาตให้ใช้เครื่องได้ แต่ส่วนหนึ่งในโปรแกรมมีลูกเล่นที่ทำให้ผู้ใช้ทำสิ่งที่ไม่ได้รับอนุญาตให้ทำได้ อย่างเช่นการอ่านรหัสผ่านของผู้ใช้อื่น ๆ หรือการแก้ไขเปลี่ยนแปลงระเบียนในแฟ้มปกปิด

เมื่อปี 1982 F.J.Shoch และ J.A. Hupp พัฒนาโปรแกรม "หนอน" ได้สำเร็จ โปรแกรมนี้เมื่อบรรจุลงในเครื่องคอมพิวเตอร์ หรือข่ายงานคอมพิวเตอร์ มันจะสามารถหาตำแหน่งที่อยู่ใหม่ได้เอง เช่น ถ้าหากมันพบว่ามีคอมพิวเตอร์เครื่องใดในข่ายงานยังไม่มีสำเนาของตัวมันเองอยู่ในเครื่องนั้น มันก็จะก๊อปปี้ตัวมันเองไปไว้ในเครื่องนั้นซ้ำยังรู้ด้วยว่าเข้าไปอยู่ในเครื่องใดบ้างแล้ว โปรแกรม "หนอน" นี้ คิดดูแล้วก็น่ากลัวว่าจะแตกลูกแตกหลานยั้วเยี้ยออกไปได้มาก แต่อันที่จริงมันก็พอมีประโยชน์บ้าง คือเอาไว้ทดสอบข่ายงานอีเธอร์เนตได้

เมื่อเดือนพฤษภาคม 1984 A.K. Dewdney นักเขียนเรื่อง Computer Recreation ในวารสาร Scientific American ได้พิมพ์บทความเกี่ยวกับเรื่องเกม Core War หรือสงครามคอร์ออกเผยแพร่ แนวคิดของเกมนี้ก็คือพยายามกันหน่วยความจำของคอมพิวเตอร์เอาไว้จำนวนหนึ่งแล้วใช้หลักการเลขคณิตแบบ Modulo ทำให้เห็นว่าหน่วยความจำนั้นวนต่อกันเป็นวง ต่อจากนั้นก็เขียนโปรแกรมภาษาแอสเซมบลีขึ้นสองโปรแกรมให้มีจุดมุ่งหมายที่จะทำลายกันเอง เริ่มแรกก็จะบรรจุโปรแกรมทั้งสองลงในหน่วยความจำแบบสุ่มและไม่ให้ซ้อนทับกัน ต่อจากนั้นโปรแกรมทั้งสองก็พยายามจะหาตำแหน่งให้ตัวเองใหม่ โดยผลัดกันลบและซ้อนทับโปรแกรมอีกฝ่ายหนึ่งไปเรื่อย ๆ เกมสงครามคอร์นี้จะลงเอยให้ผลสองอย่าง กล่าวคือถ้าหากแต่ละโปรแกรมทำงานไปได้ N คำสั่งแล้วยังไม่สัมผัสถูกกันเลย ก็ให้ถือว่าเสมอกัน แต่ถ้าโปรแกรม



หนึ่งทำงานต่อไปไม่ได้เพราะคำสั่งของมันถูกอีกโปรแกรมเปลี่ยนแปลงไปเสียแล้ว ก็ต้องถือว่าโปรแกรมคู่ต่อสู้ชนะไป

โปรแกรมเหล่านี้แหละครับที่ทำให้เกิดแนวคิดเรื่องไวรัสคอมพิวเตอร์ ซึ่งก็ไม่ใช่อะไรอื่นหากคือโปรแกรมประเภทม้าโทรจัน ซึ่งสามารถหาตำแหน่งที่อยู่ใหม่และโจมตีโปรแกรมอื่น ๆ ได้ B.W.Burnham อธิบายลักษณะของไวรัสคอมพิวเตอร์เอาไว้ว่าเป็น "ชุดคำสั่งที่สามารถก๊อบปี้ตัวเองเข้าไปในโปรแกรมอื่น ๆ ได้" บางครั้งเมื่อโปรแกรมเจ้าบ้านทำงานก็จะไปกระตุ้นให้คำสั่งไวรัสนี้ทำงานตามไปด้วย ผลก็คือมันจะรีบก๊อบปี้ตัวเองไปไว้ยังโปรแกรมต่าง ๆ ซึ่งอาจทำให้เกิดความเสียหายได้ เช่นไปลบแฟ้มข้อมูล หรือทำให้เปลืองเวลาทำงานมากไปโดยใช่เหตุ

เมื่อปี 1984 กระทาชายนามกรว่า เฟรด โคเฮน ได้ทดลองไวรัสคอมพิวเตอร์กับเครื่อง VAX 11/750 ซึ่งทำงานใต้ระบบ UNIX ผลการทดลองห้าครั้งปรากฏว่า เวลาเฉลี่ยสำหรับไวรัสคอมพิวเตอร์ที่จะกำเริบจนถึงขั้นทำให้คอมพิวเตอร์ทำงานต่อไปไม่ได้คือ 30 นาที ส่วนเวลาที่สั้นที่สุดนั้นใช้เพียงห้านาทีเท่านั้น ผลของการทดลองทำให้ฝ่ายบริหารรู้สึกวิตกจนต้องห้ามไม่ให้ดำเนินการทดลองต่อไป เพราะเกรงว่าดีไม่ดีเจ้าคอมพิวเตอร์จะเสียเอาจริง ๆ ได้

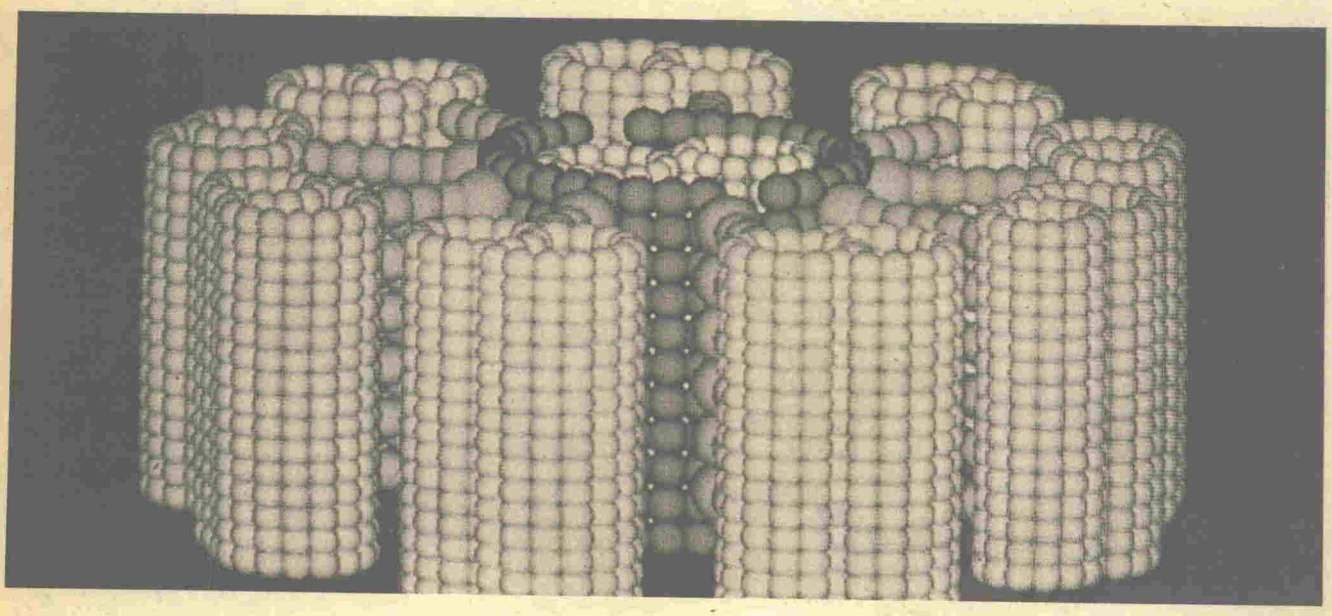
โคเฮนเล่าว่า ถ้าหากเขารู้ลักษณะการทำงานของคอมพิวเตอร์ไม่ว่าแบบใดแล้วละก็เขาสามารถที่จะสร้างไวรัสซึ่งอาจแพร่ไปยังโปรแกรมต่าง ๆ ได้จนต้องยอมให้มันทำอะไรก็ได้ภายใน 30 นาทีเท่านั้น โคเฮน ตั้งใจจะทดลองกับระบบ Tops-20 ระบบ VMS และระบบ VM/370 รวมทั้งระบบข่ายงานที่เชื่อมต่อคอมพิวเตอร์เหล่านี้ด้วยแต่ก็ไม่ได้รับอนุญาต ต่อมาเขามีโอกาสได้ทดลองกับเครื่อง UNIVAC 1108 ซึ่งติดตั้งระบบความปลอดภัยพิเศษ ซึ่งก็ปรากฏว่าไวรัสของเขาสามารถแพร่เชื้อเล่นงานเครื่องเสียงอมไปเลย

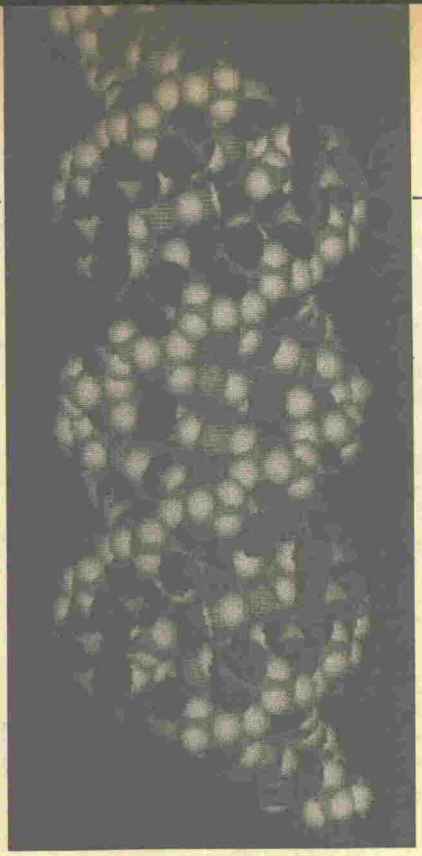
ขณะนี้ไม่มีใครทราบว่าไวรัสคอมพิวเตอร์ระบาดไปแค่ไหนแล้ว นักกฎหมายอเมริกันคนหนึ่งรายงานว่าบริษัทซอฟต์แวร์บางแห่งดำริจะบรรจุไวรัสลงในซอฟต์แวร์ที่สงวนสิทธิ์ เพื่อป้องกันการก๊อบปี้ เจ้าไวรัสนี้จะเริ่มแผลงฤทธิ์ถ้ามันรู้ว่ามีการแอบก๊อบปี้โปรแกรมนั้น เมื่อมันออกฤทธิ์แล้วมันจะเล่นงานทั้งตัวระบบ ทั้งซอฟต์แวร์และจานแม่เหล็กด้วยเมื่อข่าวนี้แพร่ออกไปบรรดาผู้ใช้คอมพิวเตอร์ก็พากันส่งจดหมายมาคัดค้าน เพราะในแง่กฎหมายลิขสิทธิ์แล้ว ผู้ใช้มีสิทธิ์ก๊อบปี้ซอฟต์แวร์เพื่อทำแผ่นสำรองได้ ถ้าหากบริษัทซอฟต์แวร์บรรจุไวรัสลงไปในซอฟต์แวร์แล้วทำให้เกิดความเสียหายขึ้น บริษัทก็อาจถูกฟ้องร้องได้

"ผลการทดลองห้าครั้งกับเครื่อง VAX 11/750 ปรากฏว่า เวลาที่สั้นที่สุดสำหรับไวรัสคอมพิวเตอร์กำเริบจนถึงขั้นทำให้คอมพิวเตอร์ทำงานต่อไปไม่ได้คือเพียง 5 นาทีเท่านั้น"

ไวรัสคอมพิวเตอร์ในเอไอที

ข่าวคราวเรื่องไวรัสคอมพิวเตอร์





ในเอไอทีนั้นเกิดขึ้นพร้อม ๆ กับที่หนังสือพิมพ์บางกอกโพสต์ลงข่าวเรื่องไวรัสในมหาวิทยาลัยเฮบรูว์ เนื้อข่าวของบางกอกโพสต์ระบุว่าไวรัสทำลายข้อมูลการวิจัยรายการบัญชี รายชื่อนักศึกษาและบรรดาข้อมูลต่าง ๆ ที่ฝ่ายบริหาร อาจารย์และนักศึกษาเก็บไว้ในระบบคอมพิวเตอร์โดยผู้ประสงค์ร้ายได้แอบบรรจุไวรัสลงในโปรแกรมด้วยวิธีธรรมดา ๆ นี้เอง โปรแกรมเมอร์ชื่อ ยิสราเอล เรดาย ระบุว่า ผู้ปล่อยไวรัสกำหนดจะทำลายแฟ้มข้อมูลให้หมดสิ้นในวันศุกร์ที่ 13 พฤษภาคม ปีนี้ อันเป็นวันกู๊ดฟรายเดย์ นั่นเอง

สำหรับที่เอไอทีนั้น เจ้าไวรัสนี้มีชื่อว่า (C) BRAIN ถ้าหากไวรัสนี้เล่นงานผู้ใดละก็จะปรากฏข้อความขึ้นบนจอภาพว่า "FAT appears to be damaged" ซึ่งหมายความว่าตารางที่บอกตำแหน่งแฟ้มข้อมูลบนแผ่นดิสก์ถูกทำลายไปเรียบร้อยแล้ว แต่ขั้นนี้ก็ยังไม่แน่นักว่าถูกทำลายโดยไอ้ตัวร้ายหรือไม่ ต้องใช้ PCTOOLS อ่านดูไฟล์อีกครั้ง ถ้าเจอะ (C) BRAIN เมื่อใดก็แปลว่าถูกเจ้าไวรัสแผลงฤทธิ์เอาจริง ๆ เข้าแล้ว

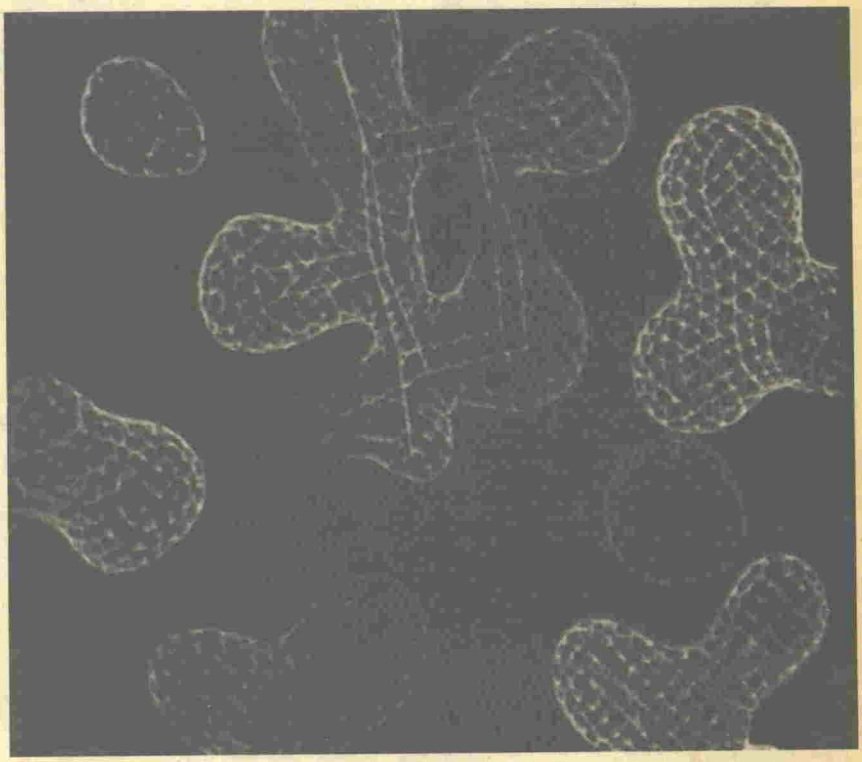
ครับ....เราก็เห็นจะต้องบอกกล่าวกันก่อนว่าแถวเอไอทีมีไวรัสระบาดแล้วนะครับ ใครจะขอก๊อบปี้โปรแกรมจากเพื่อนฝูงในเอไอทีก็ระวังกันเองก็แล้วกัน

วิธีป้องกันไวรัส

โดยที่ปัจจุบันมีไวรัสเล่นงานทั้งคอมพิวเตอร์และข่ายงานของคอมพิวเตอร์มากขึ้น ดังนั้น นักคอมพิวเตอร์จึงต้องนั่งกุมขมับหาทางป้องกันไวรัสเหล่านี้ให้ได้ มีผู้เสนอว่าในเมื่อเอาชื่อไวรัสมาเรียกโปรแกรมมหาภัยเช่นนี้ได้ มันก็ต้องมียาที่ฆ่าไวรัสได้ซีน่า ยาฆ่าไวรัสนี้ก็ไม่ใช่อะไรอื่น หากคือโปรแกรมที่จะค้นหาและทำลายโปรแกรมไวรัสเสียก่อน ปัญหาสำคัญก็คือไวรัสคอมพิวเตอร์นั้นมีหลายรูปแบบ ดังนั้น ยาขนานเดียวคงไม่อาจทำลายไวรัสได้หมดทุกประเภท ทั้งฝ่ายที่ชอบสร้างโปรแกรมไวรัสก็คงสามารถสร้างไวรัสแบบใหม่ ๆ ได้เร็วกว่าฝ่ายที่สร้างยาแก้ด้วย ยิ่งไปกว่านั้นเมื่อไวรัสกำเริบแล้ว ก็คงจะต้องใช้ทรัพยากรเครื่องจำนวนมากสำหรับต่อสู้กับไวรัส ในการต่อสู้นี้ถึงแม้เครื่องจะไม่ปราชัย ก็คงไม่อาจทำงานอื่น ๆ ได้เต็มที่

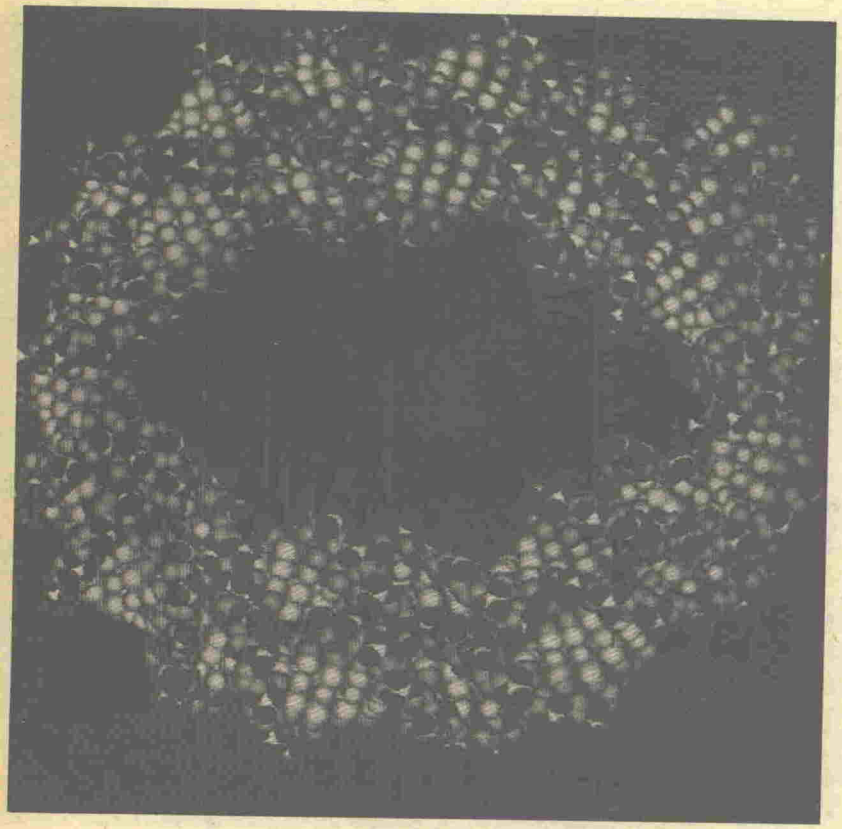
นักคอมพิวเตอร์ชื่อ อาร์.แอล.เราธ์ ได้กล่าวถึงวิธีการต่าง ๆ ที่ใช้ป้องกันระบบคอมพิวเตอร์ไม่ให้ถูกโจมตีได้ มีอาทิ การแยกระบบไว้ต่างหาก การกำหนดรายชื่อผู้ได้รับอนุมัติให้ใช้ระบบ การใช้รหัสผ่านและการลงรหัส การกำหนดโดเมนป้องกัน และการใช้ระบบอ้างอิงความสามารถ โดยที่วิธีป้องกันเหล่านี้ล้วนแต่มีปัญหาและจุดอ่อนทั้งนั้น เราธ์จึงเสนอวิธีป้องกันขึ้นมาอีกวิธีหนึ่ง ซึ่งเขาอ้างว่าอย่างน้อยก็สามารถแก้ปัญหาต่อไปนี้ได้ คือ ช่วยป้องกันปัญหาการเจาะเข้าสู่ระบบของผู้ใช้ที่มีความสามารถสูงช่วยป้องกันปัญหาม้าโทรจัน ช่วยป้องกันการเจาะเข้าไปเปลี่ยนแปลงฐานข้อมูลโดยผู้ที่ไม่ได้รับอนุญาต และปัญหาการสูญเสียกุญแจของระบบอ้างอิงความสามารถ

วิธีการของเราธ์นี้ใช้การแก้ใน



ระดับสถาปัตยกรรม คือนำระบบอ้างอิงความสามารถไปบรรจุไว้ในฮาร์ดแวร์ ซึ่งผู้ใช้ไม่อาจเข้าถึงได้ ฮาร์ดแวร์ส่วนนี้มีหน่วยความจำของตนเองซึ่งมีแต่ตัวมันเองเท่านั้นที่จะเข้าถึงได้ เรารู้ว่าโดยปกติคำสั่งทั่วไปนั้นเมื่อแปลเป็นภาษาสัญลักษณ์จะได้หลายคำสั่ง สมมติว่าแต่ละคำสั่งมีความยาว 48 บิต วิธีการของเราธ์จะสร้าง identifier ยาว 16 บิต แล้วนำไปบรรจุเป็นส่วนแรกของคำสั่งแต่ละคำสั่ง โดยวิธีนี้ก็เท่ากับฮาร์ดแวร์ทำ identifier พิเศษที่มีค่าเฉพาะไปประกบติดกับคำสั่งต่าง ๆ ตามแต่ว่าแปลมาจากภาษาอะไร ทุกคำสั่งจะผ่านกระบวนการเช่นนี้ และฮาร์ดแวร์จะเก็บรายการ identifier เหล่านี้เอาไว้ในหน่วยความจำของมัน ต่อจากนั้นจึงเป็นบิตที่แสดงลักษณะคำสั่งหรือข้อมูลซึ่งก็คือ "ความสามารถ" หรือ Capability นั่นเอง ถัดไปจึงเป็นตัวคำสั่งที่แท้จริงยาว 24 บิต และเป็นส่วนที่ซอฟต์แวร์ทั้งหลายจะเข้าถึงได้

เมื่อใช้วิธีนี้แล้ว เราก็สามารถทำงานในเครื่องที่มีไวรัสโดยที่ไวรัสทำอะไรเราไม่ได้ทั้งนี้เพราะเวลาคอมพายล์โปรแกรม ฮาร์ดแวร์จะใช้หน่วยความจำของมันสร้างตารางรักษาความปลอดภัยขึ้นสำหรับเก็บค่าในสองฟิลด์แรกของคำสั่ง รวมกับฟิลด์สุดท้ายแล้วใช้รีจิสเตอร์สำหรับบอกขอบเขตของโปรแกรมเข้าช่วยด้วย ค่าเหล่านี้โปรแกรมของผู้ใช้เข้าไม่ถึงและไม่อาจรู้ได้ ดังนั้น พอถึงจุดที่มันทำตามคำสั่งที่เป็นไวรัส มันก็ไม่สามารถหาหน่วยความจำของโปรแกรมอื่นที่จะแพร่เชื้อไปได้ เพราะฮาร์ดแวร์จะตรวจจับได้เสียก่อนว่ามีผู้พยายามจะออกไปนอกขอบเขตของโปรแกรมของตน หรือถ้าหากเกิดความผิดพลาดขึ้นทำให้โปรแกรมทำงานออกนอกขอบเขตไปได้ ก็จะไม่สามารถก๊อบปี้ตัวมันเข้าไว้ในโปรแกรมอื่นเพราะรหัส ID ของคำสั่งนั้นจะต่างไปจากรหัสที่เก็บเอาไว้ในตารางรักษาความปลอดภัย



"สำหรับที่เอ ไอทีนั้น หากไวรัสนี้เล่นงานผู้ใดละก็จะปรากฏข้อความขึ้นบนจอภาพว่า "FAT appears to be damaged"

ข้อเสนอแนะของเราธ์นี้ยังไม่ได้มีการทดสอบเต็มที่ เท่าที่พิจารณาดูก็มีข้อบกพร่องอยู่บ้าง เช่นต้องสิ้นเปลืองเวลามากขึ้นเพื่อตรวจสอบทุกคำสั่งก่อนการทำงานทุกครั้ง ทั้งยังสิ้นเปลืองหน่วยความจำอีกมากสำหรับเก็บตารางรักษาความปลอดภัย และถ้าเป็นระบบเครื่องแบบขนานก็ยังไม่รู้ว่าจะจัดหน่วยความจำอย่างไรด้วย

แนวทางป้องกันไวรัส

โคเฮน นักปล่อยไวรัสที่กล่าวถึงมาแล้วได้ย้ำว่า ถ้าหากไม่มีกลไกสำหรับตรวจสอบและรักษาความปลอดภัยที่ดีแล้ว นโยบายใด ๆ ก็ไร้ประโยชน์ ไม่ว่าเราจะวางนโยบายห้ามการเล่นพิเรนห้ามใช้เครื่องโดยไม่ได้รับอนุญาตใด ๆ ก็จะต้องมีคนไม่สนใจนโยบายเหล่านั้นจนได้ เดวิสและแกนเทนไบน์เจ้าของบทความนี้จึงได้เสนอแนะกลไกซึ่งเขาเชื่อว่าดีกว่าวิธีของเราธ์ เพราะไม่ต้องเปลี่ยนแปลงลักษณะคำสั่งของเครื่อง ดังนั้นจึงไม่สิ้นเปลืองเวลามากกว่าเดิม และไม่ต้องใช้หน่วยความจำมากด้วย

แนวทางนี้ก็คือการบรรจุแกนกลางของระบบปฏิบัติการและ "เจ้าหน้าที่รักษาความปลอดภัย" ลงไปในชิพ โดยให้แต่ละส่วนมีหน่วยความจำพิเศษของมันเองแยกจากของหน่วยความจำหลักหรือของอุปกรณ์รอบข้างอื่น ๆ หน่วยความจำนี้จะต้องสร้างขึ้นภายในชิพในแบบที่ไม่มีซอฟต์แวร์ใดที่กำลังทำงานอยู่จะเข้าถึงหรือเปลี่ยนแปลงค่าในหน่วยความจำนี้ได้ ที่ต้องใช้วิธีที่เรียกว่า hard-coding นี้ก็เพราะไม่มีวิธีอื่นใดที่จะรับประกันได้ว่าจะป้องกันการเปลี่ยนแปลงหรือเข้าถึงส่วนนี้ได้โดยไม่ได้รับอนุญาตนั่นเอง

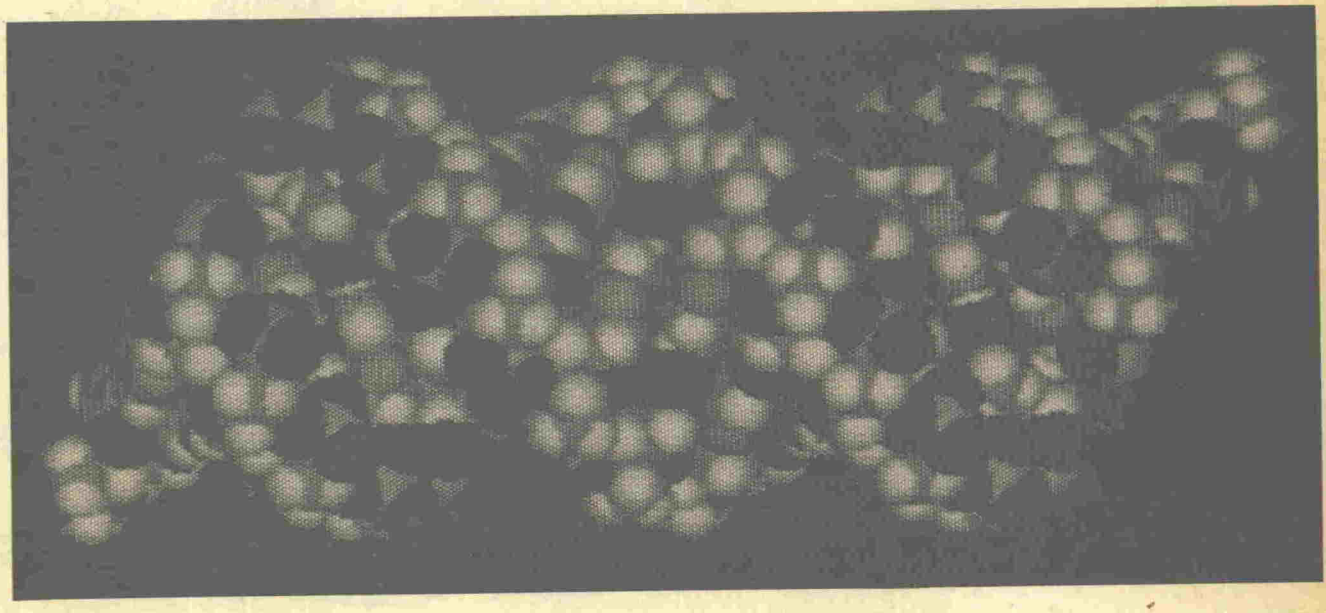
แกนกลางที่บรรจุในชิพนี้จะทำให้คอมพิวเตอร์ยังทำงานอยู่ได้ในระดับหนึ่ง แม้ว่าโปรแกรมสำคัญ ๆ อื่น ๆ จะติดเชื้อไวรัสเข้าไปแล้ว โดยเฉพาะอย่างยิ่งโปรแกรม "เจ้าหน้าที่รักษาความปลอดภัย" ที่เก็บในชิพนี้จะยังทำงานได้ ซึ่งหน้าที่ของมันก็คือตรวจหาโปรแกรมเถื่อนและป้องกันไม่ให้แพร่ลุกลามไปยังส่วนอื่น ๆ ของระบบ ทั้งยังมีส่วนที่ใช้ปราบปรามทำลายคำสั่งแปลกปลอมเหล่านั้นออกจากเครื่อง ดังนั้น เป้าหมายของการนำแกนกลางของระบบปฏิบัติการและ "เจ้าหน้าที่รักษาความปลอดภัย" มาไว้ในชิพก็เพื่อทำลายไวรัสคอมพิวเตอร์นั่นเอง

แนวทางที่ใช้ในวิธีนี้ก็คือคำนวณ "security checksum" แล้วผนวกเข้าไปกับทุกโปรแกรมนั่นเอง ค่าของ security checksum หรือผลบวกปลอดภัยก็คือจำนวนบิตที่โปรแกรมต้องการใช้เป็นที่อยู่ในหน่วยความจำนั่นเอง ค่านี้เราต้องหาให้หมดไม่ว่าจะเป็นโปรแกรมในระบบปฏิบัติการ โปรแกรมที่ใช้วิธี hard-coding และโปรแกรมของผู้ใช้ทุกโปรแกรม ค่าเหล่านี้จะเก็บไว้ในหน่วยความจำพิเศษของเจ้าหน้าที่รักษาความปลอดภัย และในตัวโปรแกรมเอง เมื่อนำโปรแกรมมาทำงาน ก็จะมีการคำนวณค่านี้ใหม่ และตรวจสอบกันค่าที่เก็บไว้แล้วเพื่อเพิ่มการป้องกันให้รัดกุมขึ้นไปอีกขั้นหนึ่ง ก็อาจจะเข้ารหัสค่าที่เก็บเอาไว้ใช้ตรวจสอบเสียก่อนก็ได้

นอกจากนั้น เมื่อทำงานเสร็จแล้วก็อาจคำนวณค่าออกมาตรวจสอบใหม่ก็ได้

ความจริงการที่ต้องทำเช่นนี้ หรือการที่เกิดมีโรคไวรัสระบาดในระบบคอมพิวเตอร์นั้นก็เป็นผลมาจากการใช้หลักการของฟอนนอยมานน์นั่นเอง กล่าวคือภายในหน่วยความจำนั้น ข้อมูลและคำสั่งมีลักษณะเป็นเลขไบนารีที่ไม่มีความแตกต่างกัน ดังนั้น จึงเป็นไปได้ที่โปรแกรมจะเปลี่ยนแปลงตัวเองได้ เพียงแต่เราไม่ค่อยจะทำกันเท่านั้น

การตรวจสอบผลบวกปลอดภัยก่อนเริ่มทำงานตามคำสั่งในโปรแกรมก็เพื่อดูว่ามีการเปลี่ยนแปลงโปรแกรมไปก่อนเริ่มทำงานไหม ถ้ามีการเปลี่ยนแปลงก็แสดงว่าเกิดไวรัสขึ้นแล้ว และเจ้าหน้าที่รักษาความปลอดภัยในชิพจะเตือนผู้ดูแลระบบให้รู้ตัวและรีบจัดการแก้ไขทันที หรือถ้าโปรแกรมทำงานเสร็จแล้ว จึงพบว่า ค่าผลบวกปลอดภัย



ไม่ตรงกับค่าที่เก็บเอาไว้ ซึ่งแสดงว่าโปรแกรมถูกเปลี่ยนแปลงไปในระหว่างการทำงาน เมื่อเกิดเหตุการณ์เช่นนี้ขึ้น ทางฝ่ายเจ้าหน้าที่รักษาความปลอดภัยก็จะเตือนให้ผู้ดูแลเครื่องทราบว่าเกิดผิดปกติแล้ว ซึ่งทางฝ่ายผู้ดูแลก็อาจตรวจสอบได้โดยการทำ back-up ของโปรแกรมเดิมก่อนการทำงานมาตรวจสอบว่ามีอะไรผิดแผกแตกต่างไปบ้าง และส่วนที่เปลี่ยนไปนั้นจะเป็นไวรัสคอมพิวเตอร์หรือไม่

วิธีป้องกันไวรัสแบบนี้ สนใจที่จะตรวจจับการแพร่เชื้อไวรัสเข้าไปในโปรแกรมที่กำลังทำงานอยู่เท่านั้น ไม่ได้ตรวจการทำลายโปรแกรมในจานแม่เหล็ก หรือป้องกันการนำโปรแกรมที่เป็นไวรัสเข้าเครื่อง ยกตัวอย่างเช่น ผมอาจคิดวิธีเขียนโปรแกรมที่เป็นไวรัสโดยใช้ editor ธรรมดา เครื่องก็จะยังคงคำนวณผลบวกความปลอดภัยให้เหมือนโปรแกรมปกติ แต่พอนำไปทำงานมันก็ยังแผลงฤทธิ์ได้ ถ้าหากมันแผลงฤทธิ์กับตัวเองแล้วละก็เจ้าหน้าที่รักษาความปลอดภัยก็คงจะตรวจจับได้ แต่มันก็มีโอกาสทำลายคำสั่งโปรแกรมอื่นได้โดยตัวเองไม่ถูกตรวจจับได้เช่นกัน สมมติว่าเราทำงานแบบมัลติโปรแกรมมิง แล้วโปรแกรมไวรัสไปทำลายโปรแกรมอื่น เมื่อโปรแกรมที่รับเชื้อไปจบงานแล้วก็จะถูกตรวจจับได้แต่โปรแกรมที่ตัวแพร่เชื้อยังอยู่อย่างเดิม และอาจคอยเล่นงานโปรแกรมอื่น ๆ ได้ต่อไป

ปัญหาสำคัญของวิธีนี้ก็คือการใช้งาน เวลาเราหาที่ผิดในโปรแกรม เราต้องมีการเปลี่ยนแปลงโปรแกรมอยู่เสมอ ก็ถ้าโปรแกรมมีขนาดมีคำสั่งเปลี่ยนแปลงไปอย่างนี้ เจ้าหน้าที่รักษาความปลอดภัยจะมิคิดว่าเกิดไวรัสขึ้นหรือไร ทั้ง ๆ ที่ความจริงก็เป็นโปรแกรมธรรมดา ๆ นี่เอง คำตอบก็คือเมื่อมีการใช้ editor เปลี่ยนแปลงโปรแกรมนั้น จะต้องมีการคำนวณผลบวกความปลอดภัยใหม่ทุกครั้ง และต้องนำไปปรับปรุงค่าที่เก็บไว้ในหน่วยความจำของเจ้าหน้าที่รักษาความปลอดภัยเสมอ รวมแล้วก็ไม่ใช่เรื่องที่ง่ายนัก

ท่านผู้อ่านอาจนึกสงสัยว่า ทำไมจึงนำแค่แกนกลางของระบบปฏิบัติการไปทำเป็น hard-code บรรจุลงชิพ จะนำทั้งระบบไปบรรจุลงชิพไม่ได้หรือ คำตอบก็คือได้แต่ไม่ดี และไม่อาจป้องกันรักษาความปลอดภัยได้ด้วย สาเหตุเป็นเพราะระบบปฏิบัติการนั้นมีความซับซ้อนมาก ซึ่งแน่นอนย่อมจะมีที่ผิดพลาดอยู่มาก และต้องมีการแก้ไขเปลี่ยนแปลงเป็นประจำ ดังนั้นการนำทั้งระบบมาบรรจุในชิพจึงย่อมไม่สะดวกอย่างแน่นอน

ปัญหายังไม่หมดสิ้น

การเขียวยารักษาคอมพิวเตอร์ที่ถูกไวรัสเล่นงานนี้ไม่ใช่เรื่องสนุกเลย เอาแค่การป้องกันนั้นถ้าจะให้ได้ผลก็ต้องใช้แนวทางแก้ลงไปในฮาร์ดแวร์ ซึ่งเป็นเรื่องที่ยุ่งยากมาก ไหนจะต้องออกแบบระบบฮาร์ดแวร์ใหม่ ไหนจะต้องจัดทำซอฟต์แวร์ใหม่อีก แต่ที่สำคัญก็คือเรายังไม่อาจบอกได้ว่าวิธีที่กล่าวมานี้ใช้ได้ผลหรือไม่

แม้จะใช้วิธีดังกล่าวก็ได้ ก็ไม่แน่ว่าจะกำจัดปัญหาต่าง ๆ ได้หมด เช่นการใช้เจ้าหน้าที่รักษาความปลอดภัยนั้น แม้จะใช้ปราบไวรัสได้ แต่ก็ไม่สามารถป้องกันการใช้เครื่องโดยไม่ได้รับอนุญาตได้ หรือในการบรรจุแกนกลางของระบบปฏิบัติการและโปรแกรมเจ้าหน้าที่รักษาความปลอดภัยลงในชิพนั้น เราจะตรวจให้แน่ใจได้อย่างไรว่าโปรแกรมเหล่านี้ยังไม่ได้ถูกไวรัสคุกคาม

ครับ...คิดดูแล้วก็เป็นปัญหาที่น่าหนักใจซึ่งจะท้าทายความสามารถของนักวิจัยและหมอคอมพิวเตอร์ต่อไปอีกนาน กว่าจะค้นพบวัคซีนที่ทำงานได้ผล

"เห็นจะต้องบอกกล่าวกันก่อนว่าแถวเอไอทีมีไวรัสระบาดแล้วนะครับ ใครจะขอก๊อบปี้โปรแกรมจากเพื่อนฝูงในเอไอทีก็ระวังกันเองก็แล้วกัน"

ส่วนในเวลานี้ ผมก็ได้แต่เตือนว่าถ้าคอมพิวเตอร์ของท่านเกิดอาการไม่ชอบมาพากล ทำอะไรแปลก ๆ แสดงข้อความแปลก ๆ หรือโปรแกรมที่เคยทำงานถูกต้องเรียบร้อยดีมานับสิบ ๆ ครั้ง เกิดผิดพลาดหรือหยุดงานโดยไม่มีเหตุผลแล้วละก็ อย่ามัวนิ่งนอนใจนะครับ อาจจะมีผู้หวังร้ายเอาไวรัสมาปล่อยเข้าไปในเครื่องของท่านแล้วก็ได้

ขอให้โชคดีครับ